대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0051488
Application Number

출 원 년 월 일 : 2002년 08월 29일
Date of Application AUG 29, 2002

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 04 월 10 일

특 허 청 장
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0006
【제출일자】	2002.08.29
【국제특허분류】	H04L
【발명의 명칭】	일방향 함수를 사용하여 계층적으로 암호화하는 장치 및 방법
【발명의 영문명칭】	Apparatus and method for hierarchical encryption using one-way function
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2000-002816-9
【발명자】	
【성명의 국문표기】	최양림
【성명의 영문표기】	CHOI,Yang Lim
【주민등록번호】	710120-1830615
【우편번호】	463-060
【주소】	경기도 성남시 분당구 이매동 124 한신아파트 210동 1509호
【국적】	KR
【발명자】	
【성명의 국문표기】	최윤호
【성명의 영문표기】	CHOI,Yun Ho
【주민등록번호】	730121-1480318

【우편번호】 138-222

【주소】 서울특별시 송파구 잠실2동 주공아파트 259동 407호

【국적】 KR

【발명자】

【성명의 국문표기】 김윤상

【성명의 영문표기】 KIM,Yun Sang

【주민등록번호】 681007-1066619

【우편번호】 441-390

【주소】 경기도 수원시 권선구 권선동 1265번지 유원.보성아파트 605동 1205 호

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이영필 (인) 대리인 이해영 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	30	면	30,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	59,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 일방향 함수를 사용하여 계층적인 정보를 가진 데이터를 암호화하는 장치 및 방법에 관한 것으로, 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 소정의 제 N 계층 키를 생성하는 제 N 계층 키 생성부, 상기 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 제 N+1 계층 키 생성부, 상기 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하는 제 N 계층 데이터 암호화부, 및 상기 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 제 N+1 계층 데이터 암호화부로 구성된다.

본 발명에 따르면 어떤 단계에 있는 의미상 단편에 대한 키를 안다고 해도 상기 단계보다 낮은 깊이의 의미상 단편들에 쉽게 접근할 수 없기 때문에 계층과 관련된 해킹의 관점에서 안전하다는 효과가 있다. 또한, 어떤 단계의 의미상 단편 과 그것의 암호화 키를 수신한 경우, 상기 단계보다 더 낮은 단계의 의미상 단편 모두를 복호화할 수 있기 때문에 키 전송의 대역 폭 사용을 절약할 수 있다는 효과가 있다.

【대표도】

도 6

【명세서】

【발명의 명칭】

일방향 함수를 사용하여 계층적으로 암호화하는 장치 및 방법{Apparatus and method for hierarchical encryption using one-way function}

【도면의 간단한 설명】

도 1은 종래 미디어 데이터를 암호화하는 방법의 구조도이다.

도 2는 종래 미디어 데이터를 암호화하는 장치의 구성도이다.

도 3은 종래 미디어 데이터를 복호화하는 장치의 구성도이다.

도 4는 종래 비디오 데이터를 암호화하는 방법의 구조도이다.

도 5는 본 발명에 따른 비디오 데이터를 계층적으로 암호화하는 방법의 구조도이다.

도 6은 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 장치의 구성도이다.

도 7은 본 발명에 따른 일방향 함수를 사용하여 계층적으로 복호화하는 장치의 구성도이다.

도 8은 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 방법의 흐름도이다.

도 9는 본 발명에 따른 일방향 함수를 사용하여 계층적으로 복호화하는 방법의 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<10> 본 발명은 일방향 함수를 사용하여 계층적인 정보를 가진 데이터를 암호화하는 장치 및 방법에 관한 것이다.

<11> 디지털 형식의 미디어 데이터가 점점 더 일반화됨에 따라, 저작권의 보호가 매우 중요한 문제로 대두되고 있다. 저작권이 적절하게 보호되지 않는다면, 콘텐츠 제공자는 서비스 사업자에게 콘텐츠를 제공하려고 하지 않을 것이므로, 디지털 미디어 서비스 사업은 발전할 수 없다. 나아가, 저작권의 보호는 데이터 전체뿐만 아니라, 데이터의 조그마한 한 부분에 대해서도 이루어져야 하는 것이 원칙이다. 예를 들어, 임의의 비디오 데이터가 존재하는 경우, 상기 비디오 데이터의 한 프레임(정지 영상)에 해당하는 데이터도, 원칙적으로는 보호될 필요가 있는 것이다. 아날로그 데이터의 보호를 위해서는 매크로비젼(macrovision) 보호 방법이 대부분 사용되고 있다. 디지털 데이터의 보호를 위해서는 주로 암호를 사용하여 데이터를 암호화하는 방법을 사용하고 있다. 디지털 데이터를 암호화하는 방법에는 여러 가지 암호화 알고리즘이 사용된다. 암호화 알고리즘은 소정의 비밀키와의 XOR 연산에 기초한 단순한 알고리즘일 수도 있고, 하나의 비밀 키(대칭적) 또는 공개 비밀 키 쌍(비대칭적)을 기반으로 한 복잡한 암호화 알고리즘일 수도 있다. 현재 업계에서는, 디지털 미디어 데이터 자체의 암호화의 경우 복잡성, 편리성, 및 보안성을 감안하여 대부분 대칭적 암호화 알고리즘을 사용하고 있다. 대칭적 알고리즘은 전체 미디어 데이터를 암호화하기 위하여 하나의 키를 사용하거나, 주기적으로 변하는 여러 개의 키를 사용한다.

<12> 미디어 서비스는 더욱 더 다양한 형태로 가고 있다. 예를 들어, VOD(Video On Demand) 서비스에서 사용자는 비디오 전체를 시청하거나 다운로드하는 것을 원하지 않을 수 있다. 반면에, 비디오의 일부분(몇 개의 키 프레임 또는 30 초 정도의 키 클립)만을 시청하거나 다운로드하는 것을 원할 수 있다. 또한, 비디오의 일부분 시청 또는 다운로드 서비스를 가능케 하기 위해 국제적 표준안(예를 들면, MPEG-7)이 제정되고 있으며, 여기에는 비디오의 계층적인 조직 정보를 담고 있는 표준 비디오 내용 기술도 담고 있다. 이러한 표준화 활동의 가장 중요한 목적은 표준 메타 데이터 스펙을 기반으로 보다 더 다양한 미디어 서비스를 허락하는 것이다.

<13> 이하에서는 도면을 참조하여 종래 기술의 문제점을 살펴보기로 한다.

<14> 도 1은 종래 미디어 데이터를 암호화하는 방법의 구조도이다.

<15> 종래 미디어 데이터를 암호화하는 방법에는 단일 키 방법(11)과 다중 키 방법(12)이 있다. 단일 키 방법(11)은 하나의 키로 미디어 데이터의 전체 또는 서브 셋을 암호화하는 것이고, 다중 키 방법(12)은 여러 개의 키로 미디어 데이터의 전체 또는 서브 셋을 암호화하는 것이다. 다중 키 방법(12)에서 일반적으로 키들은 주기적으로, 또는 비 주기적으로 바뀌어 진다. 키들의 변화를 신호로 알리기 위해서는 미디어 데이터 속에 플래그를 두는 것이 일반적이다. 일반적으로 키들은 암호화되는 미디어 데이터와 중요한 관련성은 없다.

<16> 미디어 데이터는 일반적으로 대칭적인 암호를 사용하여 암호화된다. 비대칭적인 암호는 대칭적인 암호보다 키 발생을 위한 알고리즘이 훨씬 더 복잡하고 키 사이즈가 커서, 신속한 처리와 대용량의 처리가 요구되는 미디어 데이터의 암호화에 부적당하기 때문이다. 대칭적인 암호는 암호화 및 복호화에 똑 같은 비밀 키를 사용한다.

<17> 도 2는 종래 미디어 데이터를 암호화하는 장치의 구성도이다.

<18> 종래 미디어 데이터를 암호화하는 장치는 키 생성부(21), 키 버퍼(22), 데이터 암호화부(23), 키 암호화부(24), 저장부(25), 및 송신부(26)로 구성된다.

<19> 키 생성부(21)는 미디어 데이터를 암호화할 키를 발생시킨다. 키 버퍼(22)는 키들을 일시적으로 저장해 놓고 있다가, 데이터 암호화부(23) 또는 키 암호화부(24)에서 키들을 필요로 하는 시기에 키들을 제공한다. 데이터 암호화부(23)는 제공된 키를 사용하여 데이터를 암호화한다. 키 암호화부(24)는 키를 암호화한다. 저장부(25)는 암호화된 미디어 데이터와 암호화된 키를 저장한다. 송신부(26)는 암호화하여 저장된 미디어 데이터와 암호화하여 저장된 키를 송신한다.

<20> 도 3은 종래 미디어 데이터를 복호화하는 장치의 구성도이다.

<21> 종래 미디어 데이터를 복호화하는 장치는 수신부(31), 키 복호화부(32), 키 버퍼(33), 및 데이터 복호화부(34)로 구성된다.

<22> 수신부(31)는 상기 도 2의 송신부(26)로부터 송신된 암호화 상태의 데이터와 키를 수신한다. 키 복호화부(32)는 암호화된 키를 복호화한다. 키 버퍼(33)는 키들을 일시적으로 저장해 놓고 있다가, 데이터 복호화부(34)에서 키들을 필요로 하는 시기에 키들을 제공한다. 데이터 복호화부(34)는 키들을 사용하여 암호화된 데이터를 복호화한다.

<23> 상기 도 2 또는 상기 도 3과 같이, 사용된 암호가 대칭적인 것이라면, 서버와 클라이언트는 암호화와 복호화에 대한 키를 공유할 필요가 있다. 미디어 서비스 서버상에서, 미디어 데이터는 하나의 키 또는 여러 개의 키를 사용하여 암호화된다. 개별적으로 보면, 미디어의 암호화에 사용된 키는 어떤 키를 사용하여 다시 암호화된 것이다. 이어

서, 암호화된 미디어 데이터와 암호화된 키는 클라이언트에게 전송된다. 클라이언트는 암호화된 미디어 데이터와 암호화된 키를 수신한다. 이어서, 암호화된 키가 먼저 복호화된다. 암호화된 미디어 데이터는 복호화된 키를 사용하여 복호화된다.

<24> 디지털 데이터 서비스를 제공하기 위한 환경이 제대로 갖추어 진다면, 사용자가 전체 미디어 중, 몇 개의 키 프레임만을 주문하고, 상기 프레임들을 재생해본 후에, 마음에 드는 키 프레임에 해당하는 비디오만을 주문하여 볼 수 있는 서비스가 가능해진다. 이와 같은 시나리오에서는 각각의 데이터들(키 프레임, 키 클립)을 보호해야할 필요성이 생긴다. 그러나, 상기 도 2 또는 상기 도 3의 종래 미디어 데이터를 암호화 또는 복호화하는 장치는 데이터의 일부분을 주고받는 상황을 효과적으로 지원하지 못한다는 문제점이 있다. 다시 말하면, 데이터 전체에 대해 하나의 키만을 사용하여 암호화하는 경우에는 해킹이 보다 용이하게 되고, 또 여러 개의 키를 사용하는 경우에는, 키 전송에 필요한 불필요한 대역폭이나 메모리 공간을 요구하게 되는 문제점이 있다.

<25> 예를 들면, 1 시간 짜리 비디오 데이터는, 리프(leaf)가 키 프레임(key frame)들이고, 루트(root)가 전체 비디오이고, 중간 노드(intermediate node)가 키 클립들이고, 자식(child)과 부모(parent)의 관계는 서로 포함되는 것으로 정의가 되는 트리(tree) 구조로 표현될 수 있다. 상기 트리 구조에서 키 클립과 키 프레임은 전체 영상의 의미상 중요한 부분을 대표하는 요소들이 된다. 상기 트리 구조는 MPEG-7과 같은 국제 표준 규격에서도 언급되고 있다. 상기된 정보를 가지고, 더 유동적인 미디어 서비스가 가능하다. 보기로, 사용자는 비디오 전체를 보거나, 다운로드하는 것을 원하지 않을 수도 있다. 단지, 중요한 키 프레임이 들어있는 키 클립을 원할 수도 있다. 사용자는 단지 비디오의

몇 개의 프레임을 주문할 수도 있고, 몇 개의 키 클립들로 구성된 비디오의 미리 보기를 요구할 수도 있다. 그런 다음 자신이 선택한 비디오를 보기로 결정하는 것이다. 상기의 시나리오에서는 모든 비디오 조각들(키 프레임들, 키 클립들)이 보호된 방법으로 전송되어 질 필요가 있다. 그러나, 종래의 방법은 상기된 것을 잘 지지하지 못하는데, 그 이유는 종래의 방법은 비디오의 계층적인 정보를 고려하지 않기 때문이다.

<26> 도 4는 종래 비디오 데이터를 암호화하는 방법의 구조도이다.

<27> 미디어 서비스(보기로 VOD)가 미디어 데이터의 내용과 사용자의 기호를 기반으로 좀 더 다양한 형태를 취하게 됨에 따라, 여러 형태의 서비스를 지지할 수 있는 관련 미디어 데이터 암호화 방법이 필요하게 되었다. 종래 암호화 방법의 경우, 두 가지 문제가 나타난다.

<28> 첫째, 하나의 키에 의해 암호화되었을 경우 해킹에 약하다는 문제점이 있다. 다시 말해, 하나의 키로 암호화하는 방법의 경우, 키 프레임, 키 클립, 및 전체 비디오에 대한 암호화 키가 같기 때문에 일단 키 프레임 또는 키 클립의 암호화키가 사용자에게 수신되면, 전체 비디오는 키 프레임 또는 키 클립의 키로도 복호화 될 수 있기 때문에 해킹에 약하다는 문제점이 있다.

<29> 둘째, 여러 개의 키에 의해 암호화되었다고 하더라도 미디어 데이터의 계층적 정보를 기반으로 한 미디어 서비스를 잘 고려하여 암호화하지 않으면 과다한 키 전송에 필요한 넓은 대역폭을 사용하여야 한다는 문제점이 있다. 다시 말해, 여러 개의 키로 암호화하는 방법의 경우, 상기된 하나의 키 암호화 방법의 문제점을 해결하기 위해, 다른 단계에 있는 부분 비디오 데이터는 서로 다른 키들로 암호화 될 필요가 있기 때문에 넓은 대역폭의 사용이 요구된다는 문제점이 있다. 예를 들면, 임의의 비디오가 3단계의 층(키

프레임, 키 클립, 전체 비디오)으로 이루어져 있다고 생각하고, A는 키 프레임의 세트이고, B는 키 클립에서 키 프레임을 마이너스한 세트이고, C는 전체 비디오에서 키 프레임과 키 클립을 마이너스한 세트라고 하자. 상기 A를 K1로 암호화시키고, 상기 B를 K2로 암호화시키고, 상기 C를 K3로 암호화시킬 수 있다. 따라서, 키-프레임을 복호화하기 위해서는 K1이 필요하고, 키-클립들을 복호화하기 위해서는 K1과 K2가 필요하고, 비디오 전체를 복호화하기 위해서는 K1, K2, 및 K3이 필요하다. 이것은 비디오의 계층 구조를 고려해 볼 때, 불필요한 과잉의 키 전송을 요구한다는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<30> 본 발명이 이루고자 하는 기술적 과제는 계층적인 정보를 가지고 있는 데이터의 전체는 물론 부분에 대해서 효율적으로 암호화하는 장치 및 방법을 제공하는데 있다. 본 발명이 이루고자 하는 또 다른 기술적 과제는 해킹에 강하면서도 데이터 전송 대역폭이 좁게 암호화하는 장치 및 방법을 제공하는 데 있다.

【발명의 구성 및 작용】

<31> 상기 문제점을 해결하기 위한 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 소정의 제 N 계층 키를 생성하는 제 N 계층 키 생성부, 상기 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 제 N+1 계층 키 생성부, 상기 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하는 제 N 계층 데이터 암호화부, 및 상기 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 제 N+1 계층 데이터 암호화부로 구성된다.

<32> 상기 문제점을 해결하기 위한 본 발명에 따른 일방향 함수를 사용하여 계층적으로 복호화하는 장치는 소정의 제 N 계층 키를 생성하는 제 N 계층 키 생성부, 상기 제 N 계층 키를 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 제 N+1 계층 키 생성부, 상기 제 N 계층 키를 사용하여 소정의 암호화된 제 N 계층 데이터를 복호화하는 암호화 제 N 계층 데이터 복호화부, 및 상기 제 N+1 계층 키를 사용하여 소정의 암호화된 제 N+1 계층 데이터를 복호화하는 암호화 제 N+1 계층 데이터 복호화부로 구성된다.

<33> 상기 문제점을 해결하기 위한 본 발명에 따른 방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 장치는 소정의 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 계층적 암호화부와 상기 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 상기 일방향 함수에 대입하여 상기 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 상기 암호화된 제 N 계층 데이터를 복호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 상기 암호화된 제 N+1 계층 데이터를 복호화하는 계층적 복호화부로 구성된다.

<34> 상기 문제점을 해결하기 위한 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 방법은 소정의 제 N 계층 키를 생성하는 단계, 상기 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 단계, 상기 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하는 단계, 및 상기 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 단계로 구성된다.

<35> 상기 문제점을 해결하기 위한 본 발명에 따른 일방향 함수를 사용하여 계층적으로 복호화하는 방법은 소정의 제 N 계층 키를 생성하는 단계, 상기 제 N 계층 키를 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 단계, 상기 제 N 계층 키를 사용하여 소정의 암호화된 제 N 계층 데이터를 복호화하는 단계, 및 상기 제 N+1 계층 키를 사용하여 소정의 암호화된 제 N+1 계층 데이터를 복호화하는 단계로 구성된다.

<36> 상기 문제점을 해결하기 위한 본 발명에 따른 소정의 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 단계와 상기 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 상기 일방향 함수에 대입하여 상기 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 상기 암호화된 제 N 계층 데이터를 복호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 상기 암호화된 제 N+1 계층 데이터를 복호화하는 단계로 구성된다.

<37> 이하에서는 도면을 참조하여 본 발명의 바람직한 실시 예들을 상세히 설명한다.

<38> 도 5는 본 발명에 따른 비디오 데이터를 계층적으로 암호화하는 방법의 구조도이다

<39> 미디어 데이터는 비디오 데이터, 그래픽 데이터, 또는 오디오 데이터를 포괄하는 개념으로 모든 재생 가능한 데이터를 말한다. 일반적으로, 계층 정보를 담고 있는 미디어 데이터는 비디오 데이터나 오디오 데이터이다. 본 발명의 실시 예로는 비디오 데이터만을 기술하였으나, 오디오 데이터 등도 포함하여 해석하여야 할 것이다.

<40> 본 발명에 따른 비디오 데이터를 계층적으로 암호화하는 방법은 계층적인 정보를 잘 지원하기 위해 다음의 특성을 갖추고 있다. 비디오 데이터의 의미상 단편인 키 프레임, 키 클립에서 키 프레임을 마이너스한 것, 및 전체 비디오 데이터에서 키 클립 및 키 프레임을 마이너스한 것은 서로 다른 키들에 의해 암호화된다. 또한, 상기 키들은 상기 비디오 데이터의 의미상 단편의 단계를 잘 보존해야 한다. 예를 들면, 클라이언트는 비디오 데이터를 암호화하는데 사용되어지는 가장 낮은 단계의 키를 가지고, 그 보다 높은 단계의 데이터인 키 클립을 해독(복호화)할 수 있어야 한다.

<41> 본 발명은 상기 두 가지를 만족시키는 미디어 데이터 암호화 방법을 제공한다. 그리고, 본 발명은 서버/클라이언트의 요구 사항과 암호화 방법을 지지하는 블록 다이어그램을 제공한다. 일반적으로, 미디어 데이터에 대한 메타 데이터는 단지 계층적인 정보는 아니다. 즉, 많은 다른 의미상/문법상 정보가 그 안에 있으나, 본 발명에서는 단지 계층적인 정보만을 다루고자 한다.

<42> 도 6은 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 장치의 구성도이다.

<43> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 제 N 계층 키 생성부(62), 제 N+1 계층 키 생성부(63), 제 N 계층 데이터 암호화부(69), 및 제 N+1 계층 데이터 암호화부(611)로 구성된다. 여기에서 제 N 계층 데이터 및 제 N+1 계층 데이터는 미디어 데이터를 구성하는 서로 다른 계층에 속하는 데이터를 가르킨다.

<44> 제 N 계층 키 생성부(62)는 소정의 제 N 계층 키를 생성한다. 제 N+1 계층 키 생성부(63)는 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성한다. 제 N 계층 데이터 암호화부(69)는 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를

암호화한다. 제 N+1 계층 데이터 암호화부(611)는 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화한다.

<45> 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수이다. 일방향 함수의 예로는 SHA(Secure Hash Function), MD5(Message Digest Algorithm 5), Discrete Exponentiation(exponentiation module big prime number), 또는 간단한 비밀 패딩 알고리즘이 있다.

<46> 상기 N을 가장 낮은 계층의 값으로 설정하는 경우, 즉, N이 1부터 시작되고 N=1인 경우, 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이다. 즉, 제 1 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 제 2 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이다. 일반적으로, 제 1 계층 키 생성부(62)는 난수 발생기를 사용하여 제 1 계층 키를 난수로서 생성한다. 해커가 예상할 수 없는 값으로 가장 낮은 단계의 키를 정하는 것이 보안상 유리하기 때문이다. 상기의 데이터 설정 환경에서, N=2인 경우, 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터이다. 즉, 제 2 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 제 3 계층 데이터는 미디어 데이터의 키 프레임 데이터이다. 제 N 계층 키 생성부는 제 N-1 계층 키를 상기

일방향 함수에 대입하여 제 N 계층 키를 생성한다. 즉, 제 2 계층 키 생성부는 상기 제 1 계층 키를 상기 일방향 함수에 대입하여 제 2 계층 키를 생성한다.

<47> 따라서, 제 N 계층 키 생성부(62)와 제 N+1 계층 키 생성부(63)는 상기 N이 가장 낮은 계층의 값인 경우에는 상기한 바와 같이 난수로서 생성하거나, 임의적으로 사용자가 지정해주어야 하나, 그 이후의 계층에서는 일방향 함수에 대입함으로서 계속적으로 생성해준다.

<48> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 제 N 계층 키를 생성하는 시기와 생성된 제 N 계층 키를 사용하여 제 N 계층 데이터를 암호화하는 시기를 동기화하기 위하여 제 N 계층 키 버퍼(66), 제 N 계층 키 생성 명령부(61), 및 제 N 계층 키 제공 명령부(65)를 부가적 구성 요소로서 더 포함한다.

<49> 제 N 계층 키 버퍼(66)는 제 N 계층 키를 일시적으로 저장한다. 제 N 계층 키 생성 명령부(61)는 소정의 메타 데이터를 입력받은 경우, 메타 데이터에 따라 제 N 계층 키 생성부(62)에 제 N 계층 키를 생성할 것을 명령한다. 제 N 계층 키 제공 명령부(65)는 제 N 계층 데이터를 입력받은 경우, 메타 데이터에 따라 제 N 계층 키 버퍼(66)에 저장된 제 N 계층 키를 제 N 계층 데이터 암호화부(69)에 제공할 것을 명령한다. 메타 데이터는 데이터를 설명해주는 데이터로서, 데이터가 미디어 데이터인 경우 메타 데이터는 계층 정보(전체 비디오 데이터인가, 키 클립인가, 키 프레임인가)를 포함한다.

<50> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 제 N+1 계층 키를 생성하는 시기와 생성된 제 N+1 계층 키를 사용하여 제 N+1 계층 데이터를 암호화하는 시기를 동기화하기 위하여 제 N+1 계층 키 버퍼(67), 제 N+1 계층 키 생성 명령부(64), 및 제 N+1 계층 키 제공 명령부(68)를 부가적 구성 요소로서 더 포함한다.

<51> 제 N+1 계층 키 버퍼(67)는 제 N+1 계층 키를 일시적으로 저장한다. 제 N+1 계층 키 생성 명령부(64)는 소정의 메타 데이터를 입력받은 경우, 메타 데이터에 따라 제 N+1 계층 키 생성부(63)에 제 N+1 계층 키를 생성할 것을 명령한다. 제 N+1 계층 키 제공 명령부(68)는 제 N+1 계층 데이터를 입력받은 경우, 메타 데이터에 따라 제 N+1 계층 키 버퍼에 저장된 제 N+1 계층 키를 제 N+1 계층 데이터 암호화부(611)에 제공할 것을 명령한다. 메타 데이터는 데이터를 설명해주는 데이터로서, 데이터가 미디어 데이터인 경우 메타 데이터는 계층 정보(전체 비디오 데이터인가, 키 클립인가, 키 프레임인가)를 포함한다.

<52> 메타 데이터에 트리 형태의 계층적인 정보가 포함된 경우, 미디어 데이터는 소위 "의미상 단편" 인 상호 교집합이 없는 데이터 조각들로 분리된다. 데이터 조각 각각은 트리에서의 노드에 대응된다. 암호화된 미디어 데이터에 대응하는 트리의 깊이(단계)와 노드 위치를 발견하기 위하여, 메타 데이터로부터 미디어 데이터와 관련된 계층 정보를 읽는다. 상기 계층 정보에 따라 얼마나 많은 키가 연속적으로 발생될 필요가 있는 지를 키 생성부(62, 63)에 신호로 알린다. 또한, 지금 막 암호화된 미디어 데이터에 적용할 올바른 키를 출력하기 위하여 키 버퍼(66, 67)에 신호를 보낸다.

<53> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 보안을 강화하기 위하여 전송 데이터뿐만 아니라 키도 암호화하여 전송할 필요가 있다. 해커가 이미 사용자가 사용하고 있는 암호화 알고리즘을 알고 있는 경우, 키를 알아내면 암호화된 데이터를 복호화할 수 있기 때문이다. 따라서, 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 제 N 계층 키를 암호화하기 위하여 제 N 계층 키 암호화부(610)를 부가적 구성요소로서 더 포함한다. 제 N 계층 키 암호화부(610)는 제 N 계층 키를 암호화한다.

<54> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 암호화된 제 N 계층 키를 송신하기 위하여 암호화 제 N 계층 키 송신부(618)를 부가적 구성요소로서 더 포함한다. 암호화 제 N 계층 키 송신부(618)는 암호화된 제 N 계층 키를 송신한다.

<55> 키를 암호화하여 바로 송신하는 것이 아니고, 키를 일단 암호화한 후에 사용자로부터 요청이 있는 경우 송신하는 경우도 상정해 볼 수 있다. 수신기가 암호화된 데이터를 수신할 있는 상태임을 사용자가 인지한 경우에, 암호화된 데이터 및 키를 송신하는 것이 일반적이므로 후자를 고려할 필요가 있다. 따라서, 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 사용자로부터 요청이 있는 경우 송신하기 위하여 암호화 제 N 계층 키 저장부(614)와 암호화 제 N 계층 키 송신부(618)를 더 포함한다. 암호화 제 N 계층 키 저장부(614)는 암호화된 제 N 계층 키를 저장한다. 암호화 제 N 계층 키 송신부(618)는 사용자로부터 요청이 있는 경우, 암호화하여 저장된 제 N 계층 키를 송신한다.

<56> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 보안을 강화하기 위하여 전송 데이터뿐만 아니라 키도 암호화하여 전송할 필요가 있다. 해커가 이미 사용자가 사용하고 있는 암호화 알고리즘을 알고 있는 경우, 키를 알아내면 암호화된 데이터를 복호화할 수 있기 때문이다. 따라서, 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 제 N+1 계층 키를 암호화하기 위하여 제 N+1 계층 키 암호화부(612)를 부가적 구성요소로서 더 포함한다. 제 N+1 계층 키 암호화부(612)는 상기 제 N 계층 키를 암호화한다.

<57> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 암호화된 제 N+1 계층 키를 송신하기 위하여 암호화 제 N+1 계층 키 송신부(620)를 부가적 구성요소로서 더 포함한다. 암호화 제 N+1 계층 키 송신부(620)는 암호화된 제 N 계층 키를 송신한다.

<58> 키를 암호화하여 바로 송신하는 것이 아니고, 키를 일단 암호화한 후에 사용자로부터 요청이 있는 경우 송신하는 경우도 상정해 볼 수 있다. 수신기가 암호화된 데이터를 수신할 있는 상태임을 사용자가 인지한 경우에, 암호화된 데이터 및 키를 송신하는 것이 일반적이므로 후자를 고려할 필요가 있다. 따라서, 상기 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 사용자로부터 요청이 있는 경우 송신하기 위하여 암호화 제 N+1 계층 키 저장부(616)와 암호화 제 N+1 계층 키 송신부(618)를 더 포함한다. 암호화 제 N+1 계층 키 저장부(616)는 상기 암호화된 제 N+1 계층 키를 저장한다. 암호화 제 N+1 계층 키 송신부(620)는 사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N+1 계층 키를 송신한다.

<59> 상기 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 암호화된 제 N 계층 데이터를 송신하기 위하여 암호화 제 N 계층 데이터 송신부(617)를 부가적 구성요소로서 더 포함한다. 암호화 제 N 계층 데이터 송신부(617)는 상기 암호화된 제 N 계층 키를 송신한다.

<60> 데이터를 암호화하여 바로 송신하는 것이 아니고, 데이터를 일단 암호화한 후에 사용자로부터 요청이 있는 경우 송신하는 경우도 상정해 볼 수 있다. 수신기가 암호화된 데이터를 수신할 있는 상태임을 사용자가 인지한 경우에, 암호화된 데이터 및 키를 송신하는 것이 일반적이므로 후자를 고려할 필요가 있다. 따라서, 상기 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 사용자로부터 요청이 있는 경우 송신하기 위하여 암호화 제 N 계층 데이터 저장부(613)와 암호화 제 N 계층 데이터 송신부(617)를 더 포함한다. 암호화 제 N 계층 데이터 저장부(613)는 상기 암호화된 제 N 계층 데이터를 저장

한다. 암호화 제 N 계층 데이터 송신부(617)는 사용자로부터 요청이 있는 경우, 암호화하여 저장된 제 N 계층 데이터를 송신한다.

<61> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 암호화된 제 N+1 계층 데이터를 송신하기 위하여 암호화 제 N+1 계층 데이터 송신부(619)를 부가적 구성요소로서 더 포함한다. 암호화 제 N+1 계층 데이터 송신부(619)는 상기 암호화된 제 N 계층 키를 송신한다.

<62> 데이터를 암호화하여 바로 송신하는 것이 아니고, 데이터를 일단 암호화한 후에 사용자로부터 요청이 있는 경우 송신하는 경우도 상정해 볼 수 있다. 수신기가 암호화된 데이터를 수신할 있는 상태임을 사용자가 인지한 경우에, 암호화된 데이터 및 키를 송신하는 것이 일반적이므로 후자를 고려할 필요가 있다. 따라서, 상기 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 사용자로부터 요청이 있는 경우 송신하기 위하여 암호화 제 N+1 계층 데이터 저장부(615)와 암호화 제 N+1 계층 데이터 송신부(619)를 더 포함한다. 암호화 제 N+1 계층 데이터 저장부(615)는 상기 암호화된 제 N+1 계층 데이터를 저장한다. 암호화 제 N+1 계층 데이터 송신부(619)는 사용자로부터 요청이 있는 경우, 암호화하여 저장된 제 N 계층 데이터를 송신한다.

<63> 도 7은 본 발명에 따른 일방향 함수를 사용하여 계층적으로 복호화하는 장치의 구성도이다.

<64> 상기 일방향 함수를 사용하여 계층적으로 복호화하는 장치는 제 N 계층 키 생성부(72), 제 N+1 계층 키 생성부(73), 암호화 제 N 계층 데이터 복호화부(79), 및 암호화 제 N+1 계층 데이터 복호화부(710)로 구성된다.

<65> 제 N 계층 키 생성부(72)는 소정의 제 N 계층 키를 생성한다. 제 N+1 계층 키 생성부(73)는 제 N 계층 키를 일방향 함수에 대입하여 제 N+1 계층 키를 생성한다. 암호화 제 N 계층 데이터 복호화부(79)는 제 N 계층 키를 사용하여 소정의 암호화된 제 N 계층 데이터를 복호화한다. 암호화 제 N+1 계층 데이터 복호화부(710)는 제 N+1 계층 키를 사용하여 소정의 암호화된 제 N+1 계층 데이터를 복호화한다.

<66> 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수이다. 송신기와 수신기 양쪽에 공통되는 일방향 함수를 어떠한 방법으로 채용하는 것이 보안상 유리한 지가 문제가 된다. 일반적으로 공통적인 일방향 함수는 생산 단계에서 송수신기에 직접 탑재되거나, 송수신기에 보호 방법으로 다운로드될 수 있다.

<67> 상기 N을 가장 낮은 계층의 값으로 설정하는 경우, 즉, N이 1부터 시작되고 N=1인 경우, 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이다. 즉, 제 1 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 제 2 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이다. 일반적으로, 제 N 계층 키 생성부(72)는 상기 제 N 계층 키를 수신하여 제 N 계층 키를 생성한다. 즉, 제 N 계층 키 생성부(72)는 소정의 암호화된 제 N 계층 키를 수신하는 암호화 제 N 계층 키 수신부(721)와 수신된 암호화 제 N 계층 키를 복호화하여 제 N 계층 키를 생성하는 암호화 제 N 계층 키 복호화부(722)로 구성된다. 일반

적으로, 수신된 신호는 암호화된 데이터와 암호화된 키를 모두 포함한다. 암호화된 키를 수신된 신호로부터 분리하여 복호화한다.

<68> 상기의 데이터 설정 환경에서, N=2인 경우, 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터이다. 즉, 제 2 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 제 3 계층 데이터는 미디어 데이터의 키 프레임 데이터이다. 제 N 계층 키 생성부(72)는 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성한다. 즉, 제 2 계층 키 생성부는 상기 제 1 계층 키를 상기 일방향 함수에 대입하여 제 2 계층 키를 생성한다.

<69> 따라서, 제 N 계층 키 생성부(72)와 제 N+1 계층 키 생성부(73)는 상기 N이 가장 낮은 계층의 값인 경우에는 상기한 바와 같이 소정의 암호화된 키를 수신한 후, 복호화하여 생성하나, 그 이후의 계층에서는 일방향 함수에 대입함으로서 계속적으로 생성해준다.

<70> 일방향 함수를 사용하여 계층적으로 복호화하는 장치는 제 N 계층 키를 생성하는 시기와 생성된 제 N 계층 키를 사용하여 제 N 계층 데이터를 암호화하는 시기를 동기화하기 위하여 제 N 계층 키 버퍼(76), 제 N 계층 키 생성 명령부(71), 및 제 N 계층 키 제공 명령부(75)를 부가적 구성 요소로서 더 포함한다.

<71> 제 N 계층 키 버퍼(76)는 제 N 계층 키를 일시적으로 저장한다. 제 N 계층 키 생성 명령부(71)는 소정의 메타 데이터를 입력받은 경우, 메타 데이터에 따라 제 N 계층 키 생성부에 제 N 계층 키를 생성할 것을 명령한다. 제 N 계층 키 제공 명령부(75)는 암호화된 제 N 계층 데이터를 입력받은 경우, 메타 데이터에 따라 제 N 계층 키 버퍼에 저장

된 제 N 계층 키를 암호화 제 N 계층 데이터 복호화에 제공할 것을 명령한다. 메타 데이터는 데이터를 설명해주는 데이터로서, 데이터가 미디어 데이터인 경우 메타 데이터는 계층 정보(전체 비디오 데이터인가, 키 클립인가, 키 프레임인가)를 포함한다.

<72> 일방향 함수를 사용하여 계층적으로 암호화하는 장치는 제 N+1 계층 키를 생성하는 시기와 생성된 제 N+1 계층 키를 사용하여 제 N+1 계층 데이터를 암호화하는 시기를 동기화하기 위하여 제 N+1 계층 키 버퍼(77), 제 N+1 계층 키 생성 명령부(74), 및 제 N+1 계층 키 제공 명령부(78)를 부가적 구성 요소로서 더 포함한다.

<73> 제 N+1 계층 키 버퍼(77)는 제 N+1 계층 키를 일시적으로 저장한다. 제 N+1 계층 키 생성 명령부(74)는 소정의 메타 데이터를 입력받은 경우, 메타 데이터에 따라 제 N+1 계층 키 생성부에 제 N+1 계층 키를 생성할 것을 명령한다. 제 N+1 계층 키 제공 명령부(78)는 제 N+1 계층 데이터를 입력받은 경우, 메타 데이터에 따라 제 N+1 계층 키 버퍼에 저장된 제 N+1 계층 키를 암호화 제 N+1 계층 데이터 복호화부에 제공할 것을 명령한다. 메타 데이터는 데이터를 설명해주는 데이터로서, 데이터가 미디어 데이터인 경우 메타 데이터는 계층 정보(전체 비디오 데이터인가, 키 클립인가, 키 프레임인가)를 포함한다.

<74> 도 8은 본 발명에 따른 일방향 함수를 사용하여 계층적으로 암호화하는 방법의 흐름도이다.

<75> 먼저, 소정의 제 N 계층 키를 생성한다(81). 이어서, 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성한다(82). 이어서, 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화한다(83). 이어서, 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화한다(84).

<76> 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수이다.

<77> 상기 N을 가장 낮은 계층의 값으로 설정하는 경우, 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이다. 또한, 상기 N을 가장 낮은 계층보다 한 단계 높은 계층의 값으로 설정하는 경우, 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터이다.

<78> 도 9는 본 발명에 따른 일방향 함수를 사용하여 계층적으로 복호화하는 방법의 흐름도이다.

<79> 먼저 소정의 제 N 계층 키를 생성한다(91). 이어서, 상기 제 N 계층 키를 일방향 함수에 대입하여 제 N+1 계층 키를 생성한다(92). 이어서, 상기 제 N 계층 키를 사용하여 소정의 암호화된 제 N 계층 데이터를 복호화한다(93). 이어서, 상기 제 N+1 계층 키를 사용하여 소정의 암호화된 제 N+1 계층 데이터를 복호화한다(94).

<80> 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수이다.

<81> 상기 N을 가장 낮은 계층의 값으로 설정하는 경우, 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이다. 또한, 상기 N을 가장 낮은 계층보다 한 단계 높은 계층의 값으로 설정

하는 경우, 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터이다.

<82> 한편, 상술한 본 발명의 실시 예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

<83> 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 씨디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장매체를 포함한다.

<84> 이제까지 본 발명에 대하여 그 바람직한 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

【발명의 효과】

<85> 본 발명에 따르면 어떤 단계에 있는 의미상 단편에 대한 키를 안다고 해도 상기 단계보다 낮은 깊이의 의미상 단편들에 쉽게 접근할 수 없기 때문에 계층과 관련된 해킹의 관점에서 안전하다는 효과가 있다. 또한, 어떤 단계의 의미상 단편 과 그것의 암호화 키를 수신한 경우, 상기 단계보다 더 낮은 단계의 의미상 단편 모두를 복호화할 수 있기

때문에 키 전송의 대역 폭 사용을 절약할 수 있다는 효과가 있다. 나아가, 종래의 다중 키 암호화 시스템과 비교할 때, 본 발명은 일방향 함수 계산에 의하여 더 낮은 단계의 의미상 단편들에 대한 키 암호화를 대체한다. 일반적으로 키들은 일방향 함수보다 훨씬 더 복잡한 대칭 암호로 암호화되기 때문에 전체적으로 종래의 다중 키 암호화 시스템의 복잡성을 초과하지는 않는다.

【특허청구범위】

【청구항 1】

소정의 제 N 계층 키를 생성하는 제 N 계층 키 생성부;

상기 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 제 N+1 계층 키 생성부;

상기 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하는 제 N 계층 데이터 암호화부; 및

상기 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 제 N+1 계층 데이터 암호화부를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 2】

제 1 항에 있어서, 상기 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 3】

제 1 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 4】

제 1 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 5】

제 4 항에 있어서, 상기 제 N 계층 키 생성부는 소정의 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 6】

제 1 항에 있어서,

상기 제 N 계층 키를 일시적으로 저장하는 제 N 계층 키 버퍼;

소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N 계층 키 생성부에 제 N 계층 키를 생성할 것을 명령하는 제 N 계층 키 생성 명령부; 및

상기 제 N 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N 계층 키 버퍼에 저장된 제 N 계층 키를 상기 제 N 계층 데이터 암호화부에 제공할 것을 명령하는 제 N 계층 키 제공 명령부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 7】

제 1 항에 있어서,

상기 제 N+1 계층 키를 일시적으로 저장하는 제 N+1 계층 키 버퍼;

소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N+1 계층 키 생성부에 제 N+1 계층 키를 생성할 것을 명령하는 제 N+1 계층 키 생성 명령부; 및

상기 제 N+1 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N+1 계층 키 버퍼에 저장된 제 N+1 계층 키를 상기 제 N+1 계층 데이터 암호화부에 제공할 것을 명령하는 제 N+1 계층 키 제공 명령부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 8】

제 1 항에 있어서, 상기 제 N 계층 키를 암호화하는 제 N 계층 키 암호화부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 9】

제 8 항에 있어서, 상기 암호화된 제 N 계층 키를 송신하는 암호화 제 N 계층 키 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 10】

제 8 항에 있어서,

상기 암호화된 제 N 계층 키를 저장하는 암호화 제 N 계층 키 저장부; 및

사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N 계층 키를 송신하는 암호화 제 N 계층 키 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 11】

제 1 항에 있어서, 상기 제 N+1 계층 키를 암호화하는 제 N+1 계층 키 암호화부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 12】

제 11 항에 있어서, 상기 암호화된 제 N+1 계층 키를 송신하는 암호화 제 N+1 계층 키 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 13】

제 11 항에 있어서, 상기 암호화된 제 N+1 계층 키를 저장하는 암호화 제 N+1 계층 키 저장부; 및

사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N+1 계층 키를 송신하는 암호화 제 N+1 계층 키 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 14】

제 1 항에 있어서, 상기 암호화된 제 N 계층 데이터를 송신하는 암호화 제 N 계층 데이터 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 15】

제 1 항에 있어서,

상기 암호화된 제 N 계층 데이터를 저장하는 암호화 제 N 계층 데이터 저장부; 및

사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N 계층 데이터를 송신하는 암호화 제 N 계층 데이터 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 16】

제 1 항에 있어서, 상기 암호화된 제 N+1 계층 데이터를 송신하는 암호화 제 N+1 계층 데이터 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 17】

제 1 항에 있어서,

상기 암호화된 제 N+1 계층 데이터를 저장하는 암호화 제 N+1 계층 데이터 저장부; 및

사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N+1 계층 데이터를 송신하는 암호화 제 N+1 계층 데이터 송신부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 장치.

【청구항 18】

소정의 제 N 계층 키를 생성하는 제 N 계층 키 생성부;

상기 제 N 계층 키를 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 제 N+1 계층 키 생성부;

상기 제 N 계층 키를 사용하여 소정의 암호화된 제 N 계층 데이터를 복호화하는 암호화 제 N 계층 데이터 복호화부; 및

상기 제 N+1 계층 키를 사용하여 소정의 암호화된 제 N+1 계층 데이터를 복호화하는 암호화 제 N+1 계층 데이터 복호화부를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 19】

제 18 항에 있어서, 상기 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 20】

제 18 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 21】

제 20 항에 있어서, 상기 제 N 계층 키 생성부는 상기 제 N 계층 키를 수신하여 상기 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 22】

제 20 항에 있어서, 상기 제 N 계층 키 생성부는

소정의 암호화된 제 N 계층 키를 수신하는 암호화 제 N 계층 키 수신부; 및

상기 수신된 암호화 제 N 계층 키를 복호화하여 상기 제 N 계층 키를 생성하는 암호화 제 N 계층 키 복호화부를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 23】

제 18 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 24】

제 23 항에 있어서, 상기 제 N 계층 키 생성부는 소정의 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 25】

제 18 항에 있어서,

상기 제 N 계층 키를 일시적으로 저장하는 제 N 계층 키 버퍼;

소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N 계층 키 생성부에 제 N 계층 키를 생성할 것을 명령하는 제 N 계층 키 생성 명령부; 및

상기 암호화된 제 N 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N 계층 키 버퍼에 저장된 제 N 계층 키를 상기 암호화 제 N 계층 데이터 복호화에 제

공할 것을 명령하는 제 N 계층 키 제공 명령부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 26】

제 18 항에 있어서,

상기 제 N+1 계층 키를 일시적으로 저장하는 제 N+1 계층 키 버퍼;

소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N+1 계층 키 생성부에 제 N+1 계층 키를 생성할 것을 명령하는 제 N+1 계층 키 생성 명령부; 및

상기 제 N+1 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N+1 계층 키 버퍼에 저장된 제 N+1 계층 키를 상기 암호화 제 N+1 계층 데이터 복호화부에 제공할 것을 명령하는 제 N+1 계층 키 제공 명령부를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 장치.

【청구항 27】

소정의 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 계층적 암호화부; 및

상기 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 상기 일방향 함수에 대입하여 상기 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 상기 암호화된 제 N 계층 데이터를 복호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 상기

암호화된 제 N+1 계층 데이터를 복호화하는 계층적 복호화부를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 장치.

【청구항 28】

제 27 항에 있어서, 상기 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 장치.

【청구항 29】

제 27 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 장치.

【청구항 30】

제 27 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 장치.

【청구항 31】

제 27 항에 있어서, 상기 제 N 계층 키 생성부는 소정의 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 장치.

【청구항 32】

(a) 소정의 제 N 계층 키를 생성하는 단계;

(b) 상기 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 단계;

(c) 상기 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하는 단계; 및

(d) 상기 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 단계를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 33】

제 32 항에 있어서, 상기 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 34】

제 32 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 35】

제 32 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 36】

제 35 항에 있어서, 상기 (a) 단계는 소정의 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 37】

제 32 항에 있어서,

(e) 상기 제 N 계층 키를 일시적으로 저장하는 단계;

(f) 소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 제 N 계층 키를 생성할 것을 명령하는 단계; 및

(g) 상기 제 N 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 저장된 제 N 계층 키를 상기 (c) 단계에 제공할 것을 명령하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 38】

제 32 항에 있어서,

(h) 상기 제 N+1 계층 키를 일시적으로 저장하는 단계;

(i) 소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N+1 계층 키를 생성할 것을 명령하는 단계; 및

(j) 상기 제 N+1 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 저장된 제 N+1 계층 키를 상기 (d) 단계에 제공할 것을 명령하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 39】

제 32 항에 있어서,

(k) 상기 제 N 계층 키를 암호화하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 40】

제 39 항에 있어서,

(l) 상기 암호화된 제 N 계층 키를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 41】

제 39 항에 있어서,

(11) 상기 암호화된 제 N 계층 키를 저장하는 단계; 및

(12) 사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N 계층 키를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 42】

제 32 항에 있어서,

(m) 상기 제 N+1 계층 키를 암호화하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 43】

제 42 항에 있어서,

(n) 상기 암호화된 제 N+1 계층 키를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 44】

제 42 항에 있어서,

(n1) 상기 암호화된 제 N+1 계층 키를 저장하는 단계; 및

(n2) 사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N+1 계층 키를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 45】

제 32 항에 있어서,

(o) 상기 암호화된 제 N 계층 데이터를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 46】

제 32 항에 있어서,

(o1) 상기 암호화된 제 N 계층 데이터를 저장하는 단계; 및

(o2) 사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N 계층 데이터를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 47】

제 32 항에 있어서,

(p) 상기 암호화된 제 N+1 계층 데이터를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 48】

제 32 항에 있어서,

(p1) 상기 암호화된 제 N+1 계층 데이터를 저장하는 단계; 및

(p2) 사용자로부터 요청이 있는 경우, 상기 암호화하여 저장된 제 N+1 계층 데이터를 송신하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화하는 방법.

【청구항 49】

(a) 소정의 제 N 계층 키를 생성하는 단계;

(b) 상기 제 N 계층 키를 일방향 함수에 대입하여 제 N+1 계층 키를 생성하는 단계;

(c) 상기 제 N 계층 키를 사용하여 소정의 암호화된 제 N 계층 데이터를 복호화하는 단계; 및

(d) 상기 제 N+1 계층 키를 사용하여 소정의 암호화된 제 N+1 계층 데이터를 복호화하는 단계를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 50】

제 49 항에 있어서, 상기 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 51】

제 49 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 52】

제 51 항에 있어서, 상기 (a) 단계는 상기 제 N 계층 키를 수신하여 상기 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 53】

제 51 항에 있어서, 상기 (a) 단계는

(a1) 소정의 암호화된 제 N 계층 키를 수신하는 단계; 및

(a2) 상기 수신된 암호화 제 N 계층 키를 복호화하여 상기 제 N 계층 키를 생성하는 단계를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 54】

제 49 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 55】

제 54 항에 있어서, 상기 제 (a) 단계는 소정의 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 56】

제 49 항에 있어서,

(e) 상기 제 N 계층 키를 일시적으로 저장하는 단계;

(f) 소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N 계층 키를 생성할 것을 명령하는 단계; 및

(g) 상기 암호화된 제 N 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 저장된 제 N 계층 키를 상기 (c) 단계에 제공할 것을 명령하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 57】

제 49 항에 있어서,

(h) 상기 제 N+1 계층 키를 일시적으로 저장하는 단계;

(i) 소정의 메타 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 제 N+1 계층 키를 생성할 것을 명령하는 단계; 및

(j) 상기 제 N+1 계층 데이터를 입력받은 경우, 상기 메타 데이터에 따라 상기 저장된 제 N+1 계층 키를 상기 (d) 단계에 제공할 것을 명령하는 단계를 더 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 복호화하는 방법.

【청구항 58】

(a) 소정의 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 소정의 일방향 함수에 대입하여 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 소정의 제 N 계층 데이터를 암호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 소정의 제 N+1 계층 데이터를 암호화하는 단계; 및

(d) 상기 제 N 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 상기 일방향 함수에 대입하여 상기 제 N+1 계층 키를 생성하고, 상기 생성된 제 N 계층 키를 사용하여 상기 암호화된 제 N 계층 데이터를 복호화하고, 상기 생성된 제 N+1 계층 키를 사용하여 상기 암호화된 제 N+1 계층 데이터를 복호화하는 단계를 포함하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 방법.

【청구항 59】

제 58 항에 있어서, 상기 일방향 함수는 소정의 입력 값으로부터 함수 값을 도출하는 것은 가능하나, 상기 함수 값으로부터 상기 입력 값을 도출하는 것은 불가능한 함수인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 방법.

【청구항 60】

제 58 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 전체 비디오 데이터에서 키 클립 데이터와 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 방법.

【청구항 61】

제 58 항에 있어서, 상기 제 N 계층 데이터는 미디어 데이터의 키 클립 데이터에서 키 프레임 데이터를 제거한 데이터이고, 상기 제 N+1 계층 데이터는 미디어 데이터의 키 프레임 데이터인 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 방법.

【청구항 62】

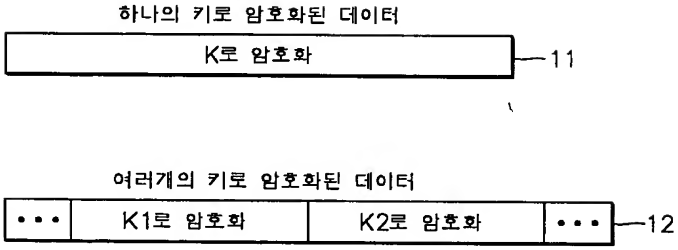
제 61 항에 있어서, 상기 (a) 단계는 소정의 제 N-1 계층 키를 상기 일방향 함수에 대입하여 제 N 계층 키를 생성하는 것을 특징으로 하는 일방향 함수를 사용하여 계층적으로 암호화 및 복호화하는 방법.

【청구항 63】

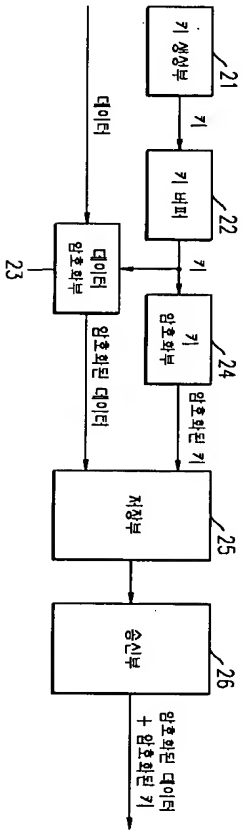
제 32 항 내지 제 62 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

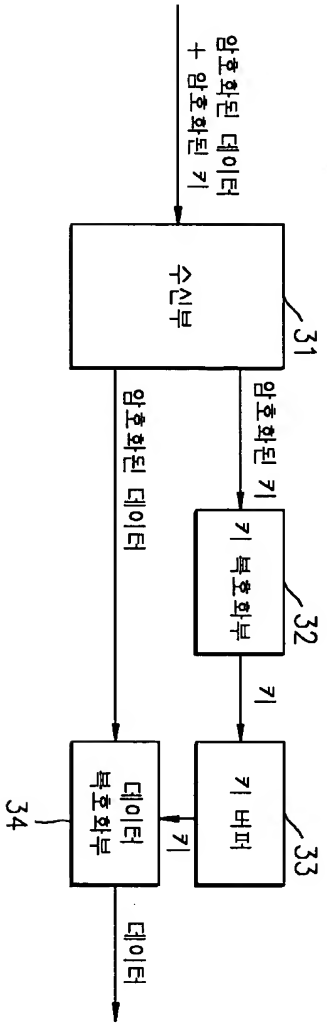
【도 1】


하나의 키로 암호화된 데이터
K로 암호화
11
여러개의 키로 암호화된 데이터
• • •
K1로 암호화
K2로 암호화
• • •
12

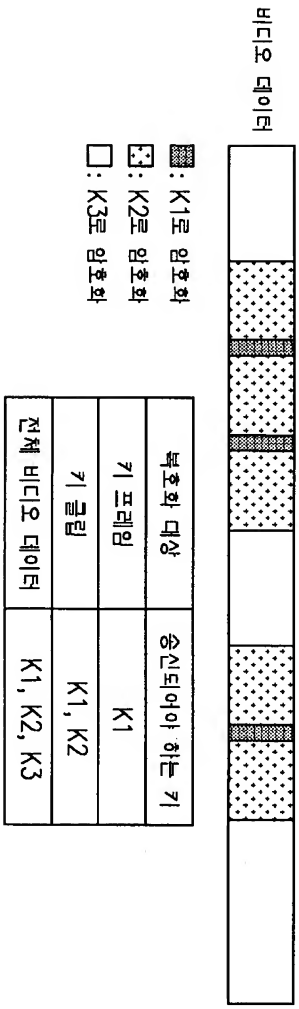
【도 2】


키 생성부
21
키
키 버퍼
22
데이터
데이터 암호화부
23
키 암호화부
24
암호화된 데이터
암호화된 키
저장부
25
송신부
26
암호화된 데이터 + 암호화된 키

【도 3】

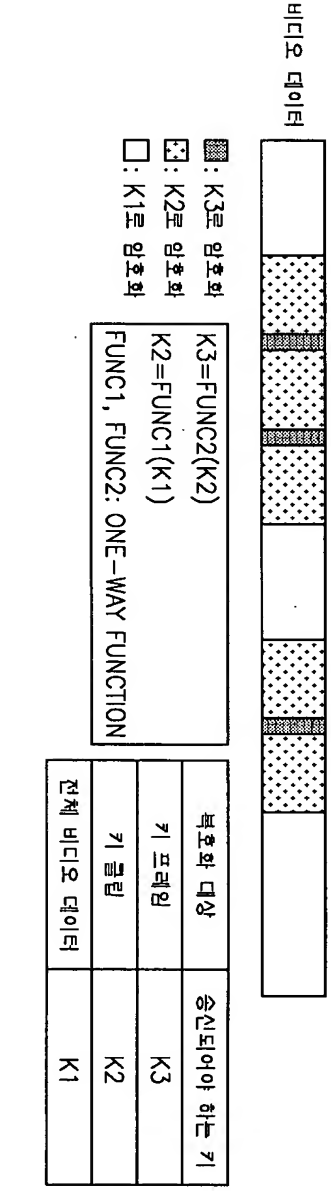

암호화된 데이터
+ 암호화된 키
수신부
31
암호화된 키
암호화된 데이터
키 복호화부
32
키
키 버퍼
33
키
데이터
복호화부
34
데이터

【도 4】

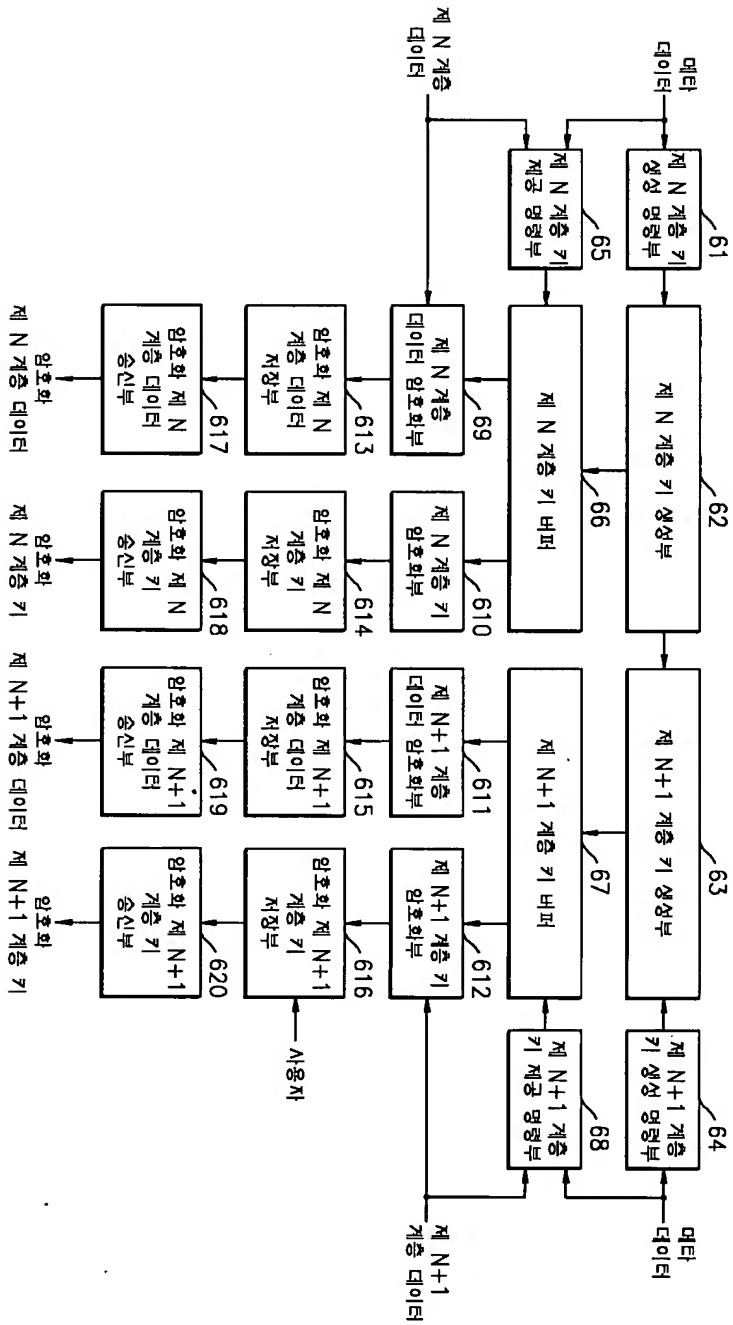


복호화 대상	송신되어야 하는 키
키 프레임	K1
키 그림	K1, K2
전체 비디오 데이터	K1, K2, K3

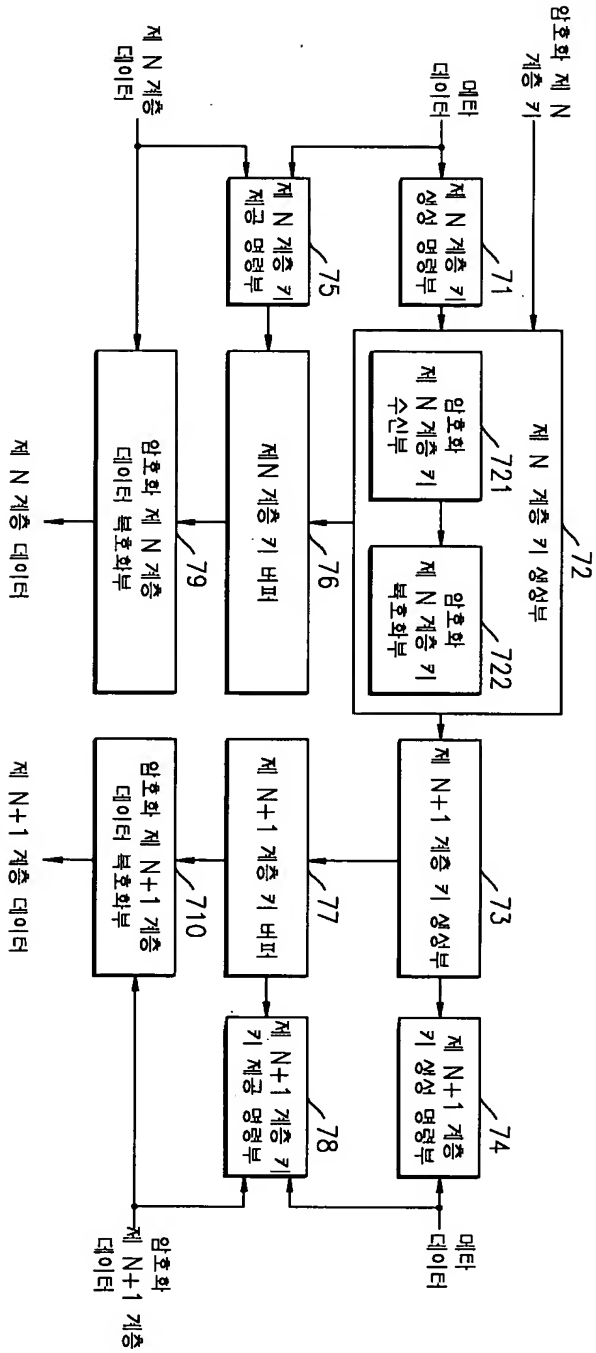
【도 5】


비디오 데이터
: K3로 암호화
: K2로 암호화
: K1로 암호화
K3=FUNC2(K2)
K2=FUNC1(K1)
FUNC1, FUNC2: ONE-WAY FUNCTION
복호화 대상
키 프레임
키 클립
전체 비디오 데이터
송신되어야 하는 키
K3
K2
K1

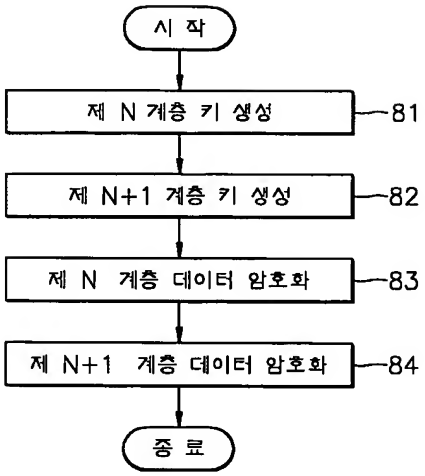
【도 6】


메타 데이터
제 N 계층 데이터
제 N 계층 키 생성 명령부
61
제 N 계층 키 제공 명령부
65
제 N 계층 키 생성부
62
제 N 계층 키 버퍼
66
제 N 계층 데이터 암호화부
69
제 N 계층 키 암호화부
610
제 N+1 계층 데이터 암호화부
611
제 N+1 계층 키 암호화부
612
제 N+1 계층 키 생성부
63
제 N+1 계층 키 버퍼
67
제 N+1 계층 키 제공 명령부
68
제 N+1 계층 키 생성 명령부
64
메타 데이터
제 N+1 계층 데이터
암호화 제 N 계층 데이터 송신부
617
암호화 제 N 계층 키 송신부
618
암호화 제 N+1 계층 데이터 송신부
619
암호화 제 N+1 계층 키 송신부
620
암호화 제 N 계층 데이터 저장부
613
암호화 제 N 계층 키 저장부
614
암호화 제 N+1 계층 데이터 저장부
615
암호화 제 N+1 계층 키 저장부
616
사용자
암호화 제 N 계층 데이터
암호화 제 N 계층 키
암호화 제 N+1 계층 데이터
암호화 제 N+1 계층 키

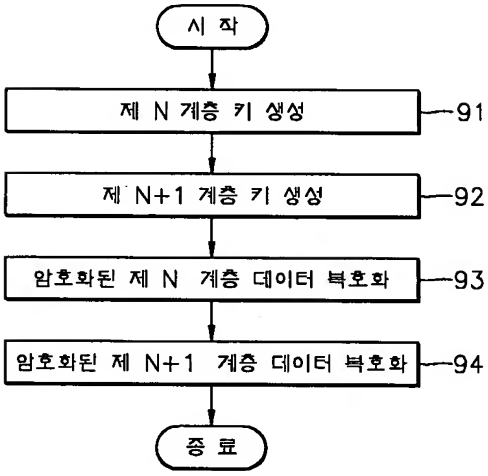
【도 7】


암호화 제 N 계층 키
메타 데이터
제 N 계층 데이터
제 N 계층 키 생성 명령부
71
제 N 계층 키 체공 명령부
75
제 N 계층 키 생성부
72
암호화 제 N 계층 키 수신부
721
암호화 제 N 계층 키 복호화부
722
제N 계층 키 버퍼
76
암호화 제 N 계층 데이터 복호화부
79
제 N 계층 데이터
제 N+1 계층 키 생성부
73
제 N+1 계층 키 버퍼
77
암호화 제 N+1 계층 데이터 복호화부
710
제 N+1 계층 데이터
제 N+1 계층 키 생성 명령부
74
제 N+1 계층 키 체공 명령부
78
메타 데이터
암호화 제 N+1 계층 데이터

【도 8】


시 작
제 N 계층 키 생성
81
제 N+1 계층 키 생성
82
제 N 계층 데이터 암호화
83
제 N+1 계층 데이터 암호화
84
종 료

【도 9】


시 작
제 N 계층 키 생성
91
제 N+1 계층 키 생성
92
암호화된 제 N 계층 데이터 복호화
93
암호화된 제 N+1 계층 데이터 복호화
94
종 료